JOURNAL OF COMBINATORIAL THEORY, Series A 32, 99–102 (1982)

Note

Eine Charakterisierung des Steinersystems $S(5, 8, 24)$

PETER HAUCK

Mathematisches Institut, Albert-Ludwigs-Universität, Albertstr. 23 b
D-7800 Freiburg i.Br, Federal Republic of Germany

Communicated by Peter Cameron

Received February 24, 1981

$S(5, 8, 24)$ is characterized as the unique Steiner system $S(t, k, n)$ satisfying $n = (t+1)(k-t+1)$ and $k \geqslant t+2 \geqslant 4$.

Ein Steinersystem $S(t, k, n)$ ist eine Menge von k-elementigen Teilmengen (den Blöcken) einer n-elementigen Menge Ω von Punkten, derart daß jede t-elementige Teilmenge von Ω in genau einem Block enthalten ist.

Bekanntlich gilt im Falle $n > k$ stets $n \geqslant (t+1)(k-t+1)$ (siehe etwa [1; Theorem 3A.5]). Es ist eine offene Frage ([1; p. 55]), welche Steinersysteme $n = (t+1)(k-t+1)$ erfüllen. Der triviale Fall $k-t+1 = 1$ (d.h. $t = n-1$) liefert gerade die Systeme $S(k, k, k+1)$. Ist $k-t+1 = 2$, so läuft obiges Problem auf die Frage nach der Existenz von Steinersystemen $S(k-1, k, 2k)$ hinaus; Beispiele dieses Typs sind nur für $k = 2$, 4 und 6 bekannt. Im folgenden Satz wird der Fall $k-t+1 > 2$ behandelt. Da für $t = 1$ nur die trivialen Systeme $S(1, k, 2k)$ auftreten, setzen wir $t \geqslant 2$ voraus.

SATZ. *Sei $S = S(t, k, n)$ ein Steinersystem mit $n = (t+1)(k-t+1)$, wobei $k \geqslant t+2 \geqslant 4$ gelte. Dann ist S das eindeutig bestimmte Steinersystem $S(5, 8, 24)$.*

Beweis. Sei $S = S(t, k, n)$ ein Steinersystem, das die Voraussetzungen des Satzes erfüllt. Zur Abkürzung sei $s = k - t + 1 = n(t+1)^{-1}$ gesetzt. Nach Voraussetzung ist $s > 2$. Wir führen den Beweis des Satzes in mehreren Schritten.

Für alle $i = 0,..., t-1$ ist $\prod_{j=0}^{i} ((t+1)(s-1)+2+j) \cdot (s+j)^{-1}$ eine ganze Zahl; insbesondere ist s ein Teiler von $t-1$: (1)

0097-3165/82/010099-04$02.00/0

Die Behauptung ergibt sich unmittelbar aus der wohlbekannten Tatsache, daß aus der Existenz eines Steinersystems $S(t, k, n)$ die Ganzzahligkeit von $\binom{n-i}{t-i} \cdot \binom{k-i}{t-i}^{-1}$ für alle $i = 0, \ldots, t-1$ folgt. Die Ganzzahligkeit von $((t+1)(s-1)+2) \cdot s^{-1}$ besagt gerade, daß s ein Teiler von $t-1$ ist.

Ist p ein Primteiler von $t+1$, so ist p ein Teiler von $s-1$ oder von $s-2$: (2)

Sei p ein Primteiler von $t+1$, welcher $s-1$ nicht teilt. Wir wählen die kleinste natürliche Zahl a mit $ap \geqslant s$. Da p kein Teiler von $s-1$ ist, ist $ap - s \leqslant p - 2 \leqslant t-1$. Nach (1) ist daher $\prod_{j=0}^{ap-s} ((t+1)(s-1)+2+j) \cdot (s+j)^{-1}$ eine ganze Zahl. Da p ein Teiler von $t+1$ ist, erzwingt dies, daß auch $\prod_{j=0}^{ap-s} (2+j) = (ap-s+2)!$ durch p teilbar ist. Dies ist aber wegen $0 < ap - s + 2 \leqslant p$ nur möglich, falls $ap - s + 2 = p$ gilt, also p ein Teiler von $s-2$ ist.

Ist p ein Primteiler von $t+1$ und von $s-1$, und ist m eine natürliche Zahl mit $p^m \leqslant t+1$, so ist p^m ein Teiler von $s-1$: (3)

Wir zeigen durch Induktion nach i, $1 \leqslant i \leqslant m$, daß p^i ein Teiler von $s-1$ ist.

Dies ist nach Voraussetzung richtig für $i = 1$. Sei also $1 < i \leqslant m$, und p^{i-1} sei ein Teiler von $s-1$. Wir nehmen an, daß $s-1$ nicht von p^i geteilt wird. Sei a die kleinste natürliche Zahl mit $ap^i \geqslant s$. Dann ist $ap^i - s \leqslant p^i - 2 \leqslant t-1$. Nach (1) ist daher $\prod_{j=0}^{r-s} ((t+1)(s-1)+2+j) \cdot (s+j)^{-1}$ eine ganze Zahl für alle $r = s, \ldots, ap^i$. Da $s-1$ von p geteilt wird, ist sicher $ap^i \geqslant s+1$. Wir zeigen zunächst, daß für alle $r = s, \ldots, ap^i - 1$ der p-Anteil von $\prod_{j=0}^{r-s} ((t+1)(s-1)+2+j)$ höchstens so groß wie der von $\prod_{j=0}^{r-s+1} (s+j)$ ist. Dies geschieht durch Induktion nach r, $s \leqslant r \leqslant ap^i - 1$. Sei zuerst $r = s$. Ist p^f die höchste p-Potenz, die in $(t+1)(s-1)+2$ aufgeht, so ist $p = 2$ und $f = 1$, denn p^2 ist ein Teiler von $(t+1)(s-1)$. Da $(s+1)s$ eine gerade Zahl ist, folgt die Behauptung.

Sei nun $s < r \leqslant ap^i - 1$. Nach Induktionsvoraussetzung genügt es zu zeigen, daß der p-Anteil von $(t+1)(s-1)+2+r-s$ höchstens so groß wie der p-Anteil von $r+1$ ist.

Sei wieder p^f die höchste p-Potenz, die in $(t+1)(s-1)+2+r-s$ aufgeht. Angenommen, $f \geqslant i$. Da p ein Teiler von $t+1$ und p^{i-1} ein Teiler von $s-1$ ist, wird folglich $2+r-s$ von p^i geteilt. Dies ist aber wegen $0 < 2+r-s \leqslant 1 + ap^i - s \leqslant p^i - 1$ nicht möglich. Mithin ist $f < i$.

Also teilt p^f sowohl $s-1$ als auch $(t+1)(s-1)+2+r-s$. Daher ist p^f auch ein Teiler von $r+1$.

Damit ist die Zwischenbehauptung bewiesen.

Da $\prod_{j=0}^{ap^i-s} ((t+1)(s-1)+2+j) \cdot (s+j)^{-1}$ ganzzahlig ist, folgt daher, daß p^i ein Teiler von $((t+1)(s-1)+2+ap^i-s) \cdot ((t+1)(s-1)+1+ap^i-s)$ ist. Aus der Teilbarkeit von $(t+1)(s-1)$ durch p^i ergibt sich somit, daß p^i in $(s-2)(s-1)$ aufgeht. Da p und $s-2$ teilerfremd sind, liefert dies, daß p^i ein Teiler von $s-1$ ist; dies widerspricht aber unserer Annahme.

Damit ist (3) bewiesen.

Ist p ein Primteiler von $s-2$, und ist p^m ein Teiler von $t+1$ für eine natürliche Zahl m, so ist p^m ein Teiler von $s-2$: (4)

Wir können o.B.d.A. $m \geqslant 2$ annehmen. Der Beweis verläuft nun ähnlich wie in (3).

Wir zeigen durch Induktion nach i, $1 \leqslant i \leqslant m$, daß p^i ein Teiler von $s-2$ ist.

Dies gilt nach Voraussetzung für $i=1$. Sei als $1 < i \leqslant m$. Wir haben die Annahme, daß p^i kein Teiler von $s-2$ ist, zum Widerspruch zu führen.

Sei a die kleinste natürliche Zahl mit $ap^i \geqslant s-1$. Dann ist $ap^i - s < p^i - 2 \leqslant t-1$ und folglich ist nach (1) $\prod_{j=0}^{r-s}((t+1)(s-1)+2+j) \cdot (s+j)^{-1}$ ganzzahlig für alle $r = s, \ldots, ap^i$. Wir zeigen zunächst, daß für alle solchen r die Zahl $\prod_{j=0}^{r-s}((t+1)(s-1)+2+j) \cdot (s+j)^{-1}$ teilerfremd zu p ist. Dies geschieht durch Induktion nach r, $s \leqslant r \leqslant ap^i$.

Sei $r=s$. Ist p^f der genaue p-Anteil von $(t+1)(s-1)+2$, so ist $p=2$ und $f=1$, da p^2 ein Teiler von $t+1$ ist. Daher ist $s-2$ gerade und damit auch s.

Sei nun $s < r \leqslant ap^i$. Nach Induktionsvoraussetzung genügt es zu zeigen, daß der p-Anteil von $(t+1)(s-1)+2+r-s$ höchstens so groß wie der p-Anteil von r ist.

Sei dazu wieder p^f die höchste p-Potenz, welche in $(t+1)(s-1)+2+r-s$ aufgeht. Da p^i ein Teiler von $t+1$ ist, ergibt sich wie in (3), daß $f < i$ gilt. Da sowohl $t+1$ als auch $s-2$ durch p^{i-1} teilbar sind, folgt somit, daß r durch p^f teilbar ist. Damit ist die Zwischenbehauptung bewiesen.

Die Ganzzahligkeit von $\prod_{j=0}^{ap^i-s}((t+1)(s-1)+2+j) \cdot (s+j)^{-1}$ hat daher zur Folge, daß $(t+1)(s-1)+2+ap^i-s$ von p^i geteilt wird. Dies erzwingt die Teilbarkeit von $s-2$ durch p^i, im Widerspruch zu unserer Annahme.

Es existiert genau ein gemeinsamer Primteiler von $t+1$ und $s-1$: (5)

Wir nehmen zunächst an, keine solche Primzahl existiere. Nach (2) und (4) ist dann $t+1$ ein Teiler von $s-2$. Ferner ist s ein Teiler von $t-1$ nach (1). Wegen $t > 1$ und $s > 2$ liefert dies den Widerspruch $t+1 \leqslant s-2 \leqslant t-3$.

Angenommen es existieren zwei gemeinsame Primteiler p und q von $t+1$ und $s-1$ mit $p > q$. Wir wählen natürliche Zahlen a und b, so daß $p^a \leqslant t+1 < p^{a+1}$ und $q^b \leqslant t+1 < q^{b+1}$ gilt. Nach (3) ist $p^a q^b$ ein Teiler von $s-1$. Wegen $p > q$ und $1 \neq s \leqslant t-1$ folgt der Widerspruch $t+1 < q^{b+1} < q^b p^a \leqslant s-1 \leqslant t-2$.

Es existiert eine Primzahl p und eine natürliche Zahl a, so daß $s = p^a + 1$ und $t + 1 = p^a(p^a - 1)$: (6)

Wegen $t \neq 1$ ist $s = (t-1) \cdot x^{-1}$ für eine natürliche Zahl x nach (1). Nach (2), (3) und (4) ist $t+1$ ein Teiler von $(s-1)(s-2)$. Wegen $s > 2$ existiert folglich eine natürliche Zahl y mit $(t+1)y = ((t-1)x^{-1} - 1) \cdot ((t-1)x^{-1} - 2)$. Dies liefert $(t+1)^2 - (x^2y + 3x + 4)(t+1) + 2x^2 + 6x + 4 = 0$. Löst man diese quadratische Gleichung nach $t+1$ auf, so ergibt sich, daß $x^2y^2 + 6xy + 8y + 1$ das Quadrat einer ganzen Zahl ist. Also ist $x^2y^2 + 6xy + 8y + 1 = (xy + v)^2$ für eine natürliche Zahl v. Dies liefert $x(2v - 6) = 8 - (v^1 - 1) \cdot y^{-1}$. Da mit $v \geqslant 3$ auch $(v^2 - 1)y^{-1} \leqslant 8$ gelten muß, lassen sich die ganzzahligen Lösungen dieser Gleichung leicht bestimmen. Man erhält die folgenden beiden Möglichkeiten:

(I) $v = 5, y = 6, x = 1$,

(II) $v = 3, y = 1$, x beliebig.

Im Fall (I) erhält man nach Einsetzen in obige quadratische Gleichung für $t+1$ die Lösungen $t = 0$ und $t = 11$. Für $t = 11$ folgt wegen $x = 1$ dann $s = 10$, $k = 20$ und $n = 120$. Da $\binom{120-7}{11-7} \cdot \binom{20-7}{11-7}^{-1}$ keine ganze Zahl ist, existiert kein Steinersystem mit diesen Parametern.

Folglich liegt Fall (II) vor, d.h. $y = 1$. Damit ist $t + 1 = (s-1)(s-2)$. Insbesondere ist $s - 1$ ein Teiler von $t + 1$ und mit (5) folgt, daß $s - 1$ eine Primzahlpotenz p^a ist.

Es ist $S = S(5, 8, 24)$: (7)

Wegen $t - 1 > 0$ ist $s(s+1)$ nach (1) ein Teiler von $((t+1)(s-1)+2) \cdot ((t+1)(s-1)+3)$. Mit (6) folgt, daß $(p^a+1) \cdot (p^a+2)$ ein Teiler von $(p^{2a}(p^a-1)+2) \cdot (p^{2a}(p^a-1)+3) = (p^a+1) \cdot (p^{2a} - 2p^a + 2) \cdot (p^{2a}(p^a-1)+3)$ ist. Da der Quotient von $(p^{2a} - 2p^a + 2)(p^{2a}(p^a-1)+3)$ und $p^a + 2$ gerade $p^{4a} - 5p^{3a} + 14p^{2a} - 27p^a + 48 - 90(p^a+2)^{-1}$ ist, erhalten wir, daß $p^a + 2$ ein Teiler von 90 ist. Damit verbleiben nur die Möglichkeiten $p^a = 3, 2^2, 7, 2^3, 13, 2^4$ und 43, aus denen sich mit Hilfe von (6) die zugehörigen Parameter t, k, n berechnen lassen. Diese verletzen jedoch, abgesehen vom Fall $p^a = 3$, die Teilbarkeitsbedingungen aus (1). Es bleibt $p^a = 3$, und man erhält $t = 5$, $k = 8$, $n = 24$. S ist somit das nach [2] eindeutig bestimmte Steinersystem $S(5, 8, 24)$.

Literatur

1. P. J. Cameron, "Parallelisms of Complete Designs," London Math. Soc. Lecture Notes 23, Cambridge Univ. Press, Cambridge, 1976.
2. E. Witt, Über Steinersche Systeme, *Abh. Math. Sem. Univ. Hamburg* **12** (1938), 265–275.